ISSN:0975-9646

Achieving Fast Recovery in IP Networks by Multiple Routing Configuration

Rajnee Kumari, Sitanath Biswas, Subrat S. Pattnaik

Dept. of Computer Science & Engineering
Gandhi Institute for Technology, Bhubaneswar, Odisha

***Abstract*-The internet has taken a central role in our communication infrastructure. The demand for internet has increased a lot but the problem is slow convergence of routing protocol after a failure has occurred. To assure a fast recovery from the link and node failures, we present new recovery scheme called multiple routing configuration (MRC).Our proposed scheme guarantees recovery from both link and node using single mechanism and without knowing root cause of the failure**.

I. INTRODUCTION

In recent years internet has become the best platform for the everyday communication services it could be a telephone conversations or TCP connections. With this the demand for internet reliability and availability has also increased .If there is disruption in link it has adverse effect on the communication especially for the real time applications.

A. Demerits of existing technology

1. Re convergence is the time consuming process and link and node failure is followed by a period of routing instability. During this period, a packet may be dropped due to invalid routes.
2. It has adverse effect on real time applications.
3. Despite of optimizing the various steps of re convergence. The convergence time is still too large for applications with real time demand.

B. Proposed scheme

MRC is a proactive and local protection mechanism that allows recovery in the range of few milliseconds. It allows packet forwarding to continue over a pre configured alternative next hops immediately after the detection of a failure. MRC can be used as first line defense against a network failure.

II. MRC OVERVIEW

MRC basically uses the network graph and associated link weights to produce small set backup configurations. MRC is basically used for short lived failure. It is used to connect the network after the failure has occurred. It is a threefold approach

1. Generating backup configurations.
2. Routing algorithm like OSPF is used to calculate configuration specific shortest path and create forwarding table in each router.
3. Design a forwarding table that take the advantage of backup configurations to provide fast recovery.

When a router detects that the neighbor has failed then it immediately does not inform the rest of network about the connectivity failure but route the packet through the backup configurations.

It is important to stress that the MRC does not affect the failure free original routing i.e. when there no failure, all packets are forwarded according to the original configuration, where all link weights are normal.

III. GENERATING BACKUP CONFIGURATION

We generate backup configuration by keeping in mind that we have to exclude a link (or groups of links) or node from taking part in routing. We observe that if all links attached to a node are given sufficiently high weights, traffic will never be routed through that node. Basically for this we must know about some of configuration structure which is as follows

TABLE 1 NOTATION

G(N,A)	Graph comprising nodes N and directed links(arcs) A.
Ci	The graph with link weights as in e configuration i
Si	The set isolated nodes in configuration Ci
Bi	The backup configuration in Ci.
A(u)	The set of links from node u.
(u, v)	The directed link from node u to node v.
Wi(u, v)	The weight of link (u, v) in configuration Ci
Wi(p)	The total weight of link paths p in configuration Ci.
Wr	The weight of a restricted link
N	The number of configurations generated

Definition - A link a ϵ A is isolated in Ci if Wi(a)= ∞.

Definition - A link a ϵ A is restricted in Ci if Wi(a)= Wr.

MRC guarantees single fault tolerance by isolating each link and node in exactly one backup configuration .A backup configuration is made by using following algorithm:

Algorithm 1: Creating backup configurations.

```
for i ∈ {1...n} do
    C_i ← (G, w_0)
    S_i ← ∅
    B_i ← C_i
end
Q_n ← N
Q_a ← ∅
i ← 1
while Q_n ≠ ∅ do
    u ← first (Q_n)
    j ← i
    repeat
        if connected(B_i \ ({u}, A(u))) then
            C_tmp ← isolate(C_i, u)
            if C_tmp ≠ null then
                C_i ← C_tmp
                S_i ← S_i ∪ {u}
                B_i ← B_i \ ({u}, A(u))
        i ← (i mod n) + 1
    until u ∈ S_i or i=j
    if u ∉ S_i then
        Give up and abort
end
```

Function `isolate` (C_i, u)

```
Q_a ← Q_a + (u, v), ∀(u, v) ∈ A(u)
while Q_a ≠ ∅ do
    (u, v) ← first (Q_a)
    if ∃j : v ∈ S_j then
        if w_j(u, v) = w_r then
            if ∃(u, x) ∈ A(u)\(u, v) : w_i(u, x) ≠ ∞ then
                w_i(u, v) ← w_i(v, u) ← ∞
            else
                return null
        else if w_j(u, v) = ∞ and i ≠ j then
            w_i(u, v) ← w_i(v, u) ← w_r
    else
        if ∃(u, x) ∈ A(u)\(u, v) : w_i(u, x) ≠ ∞ then
            w_i(u, v) ← w_i(v, u) ← ∞
        else
            w_i(u, v) ← w_i(v, u) ← w_r
            Q_n ← v + (Q_n \ v)
            Q_a ← (v, u)
end
return C_i
```

IV. LOCAL FORWARDING PROCESS

Given a sufficiently high n, the algorithm presented creates a complete set of valid backup configurations. Based on these, a standard shortest path algorithm is used in each configuration to calculate configuration specific forwarding table.

When a packet reaches a point of failure, the node adjacent to the failure, called the detecting node, is responsible for finding a backup configuration where failed component is isolated. The detecting node marks the packet belonging to this, forwards the packet with the selected backup configuration and forwards it to the destination node avoiding the failed component.

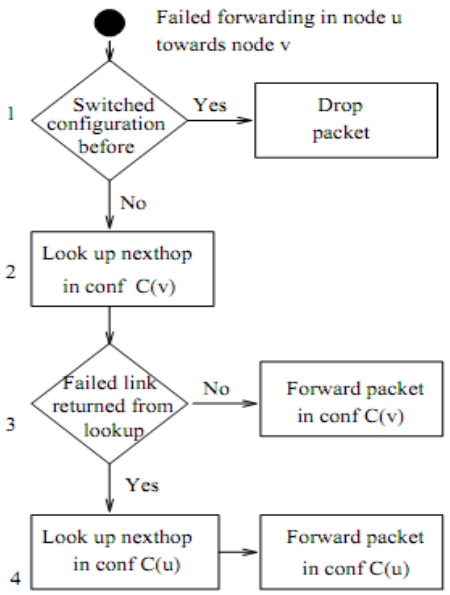

Fig packet forwarding state diagram

For a router to make correct forwarding decision, each packet must carry information about which configuration it belongs to. This information can be either explicit or implicit. An explicit approach would be using a distinct value in DSCP field of IP header to identify the configuration. A more implicit approach would tunneling but demerit with this is additional processing and bandwidth resource usage. If we can overcome this demerit then data forwarding decision could be easily by the router.

V. CONCLUSION

We have presented Multiple Routing configurations as an approach to achieve fast recovery in IP networks. MRC is based on providing the routers with additional routing configurations, allowing them to forward packets along routes that avoid a failed component. MRC guarantees recovery from any single node or link failure in an arbitrary bi-connected network. By calculating backup configurations in advance, and operating based on locally available information only, MRC can act promptly after failure discovery.

MRC operates without knowing the root cause of failure, i.e., whether the forwarding disruption is caused by a node or link failure. This is achieved by using careful link weight assignment according to the rules we have described. The link weight assignment rules also provide basis for the specification of a forwarding procedure that successfully solves the last hop problem.

REFERENCES

[1] D. D. Clark, "The design philosophy of the DARPA internet protocols,"*SIGCOMM, Computer Communications Review*, vol. 18, no. 4, pp. 106–114, Aug. 1988.

[2] A. Basu and J. G. Riecke, "Stability issues in OSPF routing," in *Proceedings of SIGCOMM*, San Diego, California, USA, Aug. 2001, pp. 225–236.

[3] C. Labovitz, A. Ahuja, A. Bose, and F. Jahanian, "Delayed Internet Routing Convergence," *IEEE/ACM Transactions on Networking*, vol. 9,no. 3, pp. 293–306, June 2001.

[4] C. Boutremans, G. Iannaccone, and C. Diot, "Impact of link failures on VoIP performance," in *Proceedings of International Workshop on Network and Operating System Support for Digital Audio and Video*,2002, pp. 63–71.

[5] D. Watson, F. Jahanian, and C. Labovitz, "Experiences with monitoring OSPF on a regional service provider network," in *ICDCS '03: Proceedings of the 23rd International Conference on Distributed Computing Systems*. Washington, DC, USA: IEEE Computer Society, 2003, pp. 204–213.

[6] P. Francois, C. Filsfils, J. Evans, and O. Bonaventure, "Achieving sub-second IGP convergence in large IP networks," *ACM SIGCOMM Computer Communication Review*, vol. 35, no. 2, pp. 35 – 44, July 2005.